



Department of Defense
INSTRUCTION

AD-A272 358



May 23, 1984
NUMBER 5240.5

2

USD(P)

SUBJECT: DoD Technical Surveillance Countermeasures (TSCM) Survey Program

References:

- (a) DoD Instruction 5200.29, subject as above, February 12, 1975 (hereby canceled)
- (b) DoD Directive 5200.26, "Defense Investigative Program," June 12, 1979
- (c) Director of Central Intelligence (DCI) Procedural Guide No. 3, "Guidance for Conducting Technical Surveillance Countermeasures Surveys"¹
- (d) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 1982, authorized by DoD Directive 5240.1, December 3, 1982
- (e) DCI Procedural Guide No. 1, "Requirements for Reporting and Testing Technical Surveillance Penetrations"¹
- (f) DCI Procedural Guide No. 2, "Requirements for Reporting and Testing Hazards"¹
- (g) DoD Directive 5111.1, "Under Secretary for Policy," October 27, 1978

A. PURPOSE

This Instruction replaces reference (a) to update policies, responsibilities, and procedures for Technical Surveillance Countermeasures (TSCM) services which is one of the counterintelligence activities within the Defense Investigative Program (reference (b)).

B. APPLICABILITY

This Instruction applies to the Office of the Secretary of Defense, the Military Departments, the Organization of the Joint Chiefs of Staff, the Unified and Specified Commands, and the Defense Agencies (hereafter referred to collectively as "DoD Components").

¹Procedural Guide Nos. 1, 2, and 3 are issued by the DCI and are available only to members of the TSCM Subcommittee.

This document has been approved for public release and sale; its distribution is unlimited.

DTIC
ELECTE
NOV 10 1993
S
A

93-26766



C. DEFINITION

TSCM Survey. A service provided by qualified personnel to detect the presence of technical surveillance devices and hazards and to identify technical security weaknesses that could aid in the conduct of a technical penetration of the surveyed facility. A TSCM survey will provide a professional evaluation of the facility's technical security posture and normally will consist of a thorough visual, electronic, and physical examination in and about the surveyed facility.

D. POLICY

It is DoD policy that all DoD Components shall share the responsibility to detect or prevent the technical penetration efforts of hostile intelligence agencies directed against the Department of Defense.

E. PROCEDURES

1. General

a. To meet the responsibility stated in section D., above, DoD Components shall implement adequate security controls over areas that require protection; conduct selectively TSCM surveys; provide TSCM services in such areas to ensure that they are devoid of technical surveillance devices; identify hazardous conditions that could facilitate technical surveillance; and identify technical security weaknesses.

b. TSCM services are highly specialized counterintelligence investigations that are particularly vulnerable to any breach in operations security. Therefore, all DoD Components that conduct or receive TSCM services are required to use all reasonable means to protect continually the operations security of the TSCM survey program.

c. TSCM services shall be conducted only by DoD TSCM personnel who meet the criteria established in enclosure 1, using the most effective equipment available. TSCM surveys and services may not be conducted by DoD personnel or DoD contractors who do not meet the requirements of this Instruction.

d. Because TSCM services are expensive and technical manpower and equipment are limited, a high degree of selectivity must be exercised in identifying areas to be surveyed.

e. No facility will qualify automatically for recurrent TSCM services. Recurrent services in a facility shall be conducted only if such services are considered appropriate by the cognizant TSCM program manager, based upon a documented threat and vulnerability assessment of the facility. Specific consideration shall be given to (1) activities of known or suspected hostile intelligence services (HIS) agents or operatives within the geographic area; (2) deterrence offered by security measures in effect at each facility; (3) sensitivity of information that is susceptible to technical exploitation; and (4) information developed through other counterintelligence operations. The frequency of approved periodic services shall be determined by the cognizant TSCM program manager for each facility based on evaluation of the foregoing data.

f. The only DoD Components authorized to conduct TSCM surveys, acquire or possess TSCM equipment, or have TSCM personnel are the U.S. Army Intelligence and Security Command, the 650th Military Intelligence Group, the U.S. Naval Investigative Service, the U.S. Marine Corps Director of Intelligence, the U.S. Air Force Office of Special Investigations, the National Security Agency/Central Security Service, the Defense Intelligence Agency, and Washington Headquarters Services.

2. Requests and their Acceptance

a. TSCM services shall be requested in accordance with procedures established by the TSCM program manager. Requests for TSCM services shall be submitted through secure means (such as classified letter or electrical message).

b. Requests for TSCM services shall be accepted only for those facilities or categories of facilities that the cognizant TSCM program manager has determined to be probable and feasible targets for technical espionage.

c. The TSCM program managers for the conducting DoD Component shall determine which facilities shall receive TSCM services, consistent with the nature of the information to be protected and the hostile technical threat peculiar to the area. The frequency of TSCM surveys of facilities that have been approved also will be determined by the TSCM program manager for the conducting Component.

d. Requests for surveys of facilities that are not used normally to discuss sensitive information and that are open to uncontrolled access by uncleared personnel shall be approved only if no other facility is available. Surveys of such facilities have proven counterproductive by having given the occupant or occupants a false sense of security and by using limited TSCM assets that could be used more productively in other, more sensitive facilities. Conferences that require discussions of sensitive information shall be held in facilities whose security is commensurate with the sensitivity of the information to be discussed. Classified presentations by DoD personnel before congressional members and staffs shall be supported as prescribed in enclosure 2.

e. Requests for recurrent TSCM services shall be evaluated by the TSCM program managers as described in paragraph E.1.e., above.

3. Conduct of TSCM Surveys. TSCM surveys shall be conducted following the general guidance of DCI Procedural Guide No. 3 (reference (c)) and procedure 5 of DoD 5240.1-R (reference (d)). In order that cross-servicing between DoD Components may be facilitated, only minor variations needed to fulfill unique customer requirements will be permitted.

4. Reporting Requirements

a. Upon completion of a TSCM survey, a complete report shall be prepared for the requester. At a minimum, the report shall include the information prescribed in enclosure 3.

b. If a penetration or technical surveillance hazard is discovered, the general guidance in DCI Procedural Guide Nos. 1 and 2 (references (e) and (f)) shall be followed. An immediate report shall be made to the Deputy Under Secretary of Defense for Policy (DUSD(P)).

5. Shipment of TSCM Equipment. Unaccompanied shipment of TSCM equipment may be accomplished via the Armed Forces Courier Service, registered U.S. Mail, or other appropriate means, at the discretion of the owning DoD Component.

6. In-Place Monitor Systems. If commanders of highly sensitive projects or facilities desire to augment the TSCM support provided within the constraints of this Instruction, in-place monitor equipment may be procured and operated for that purpose, provided such operations are coordinated with the cognizant TSCM program manager. Equipment purchase, installation, and operation shall be funded by the using DoD Component. No in-place monitor equipment may be purchased or used without prior coordination with and approval of the cognizant TSCM program manager.

7. Classification of TSCM Related Information. Information pertaining to the TSCM program shall be provided appropriate protection to preserve the integrity of the information and the program. Such information shall be classified in accordance with the DoD Components' regulatory documents. In the interest of standardization, such Component regulatory documents, at a minimum, must include the following classification guidance. Additional explanatory language or specific categories of information may be added at the discretion of the DoD Component.

a. Correspondence or documentation that shows the date and specific location of pending TSCM activity shall be classified SECRET, but be downgraded to CONFIDENTIAL upon completion of the TSCM activity, with Originating Agency Determination Required (OADR) for declassification.

b. Technical summaries and correspondence pertaining to major security vulnerabilities shall be classified SECRET, OADR for downgrading or declassification. Minor security vulnerabilities normally shall be classified CONFIDENTIAL, OADR.

c. Information that refers to the discovery or alleged discovery of a clandestine technical penetration shall be classified SECRET, OADR.

d. Information that reveals the capabilities or limitations of TSCM equipment or TSCM equipment budgets, or procurement actions, may be classified up to SECRET, OADR, depending upon the extent and sensitivity of such information.

8. TSCM Personnel and Training

a. Personnel. The nature of TSCM as a specialized counterintelligence function requires personnel who possess extensive knowledge in investigative, electronic, and construction skills. This combination of talents is necessary to conduct successfully the complex and detailed procedures associated with TSCM services. The minimum qualifications required for consideration for entry into the TSCM field are listed in enclosure 1. In addition, the selection process shall include a personal interview and evaluation by a senior technical agent.

b. Training. All DoD TSCM agents shall receive technical surveillance countermeasures training at an approved training facility to promote survey quality and to standardize operational procedures. Instruction on DoD 5240.1-R (reference (d)) and the procedures therein shall be included in the training programs of all DoD TSCM agents. DoD Components shall ensure that their TSCM personnel attend periodically refresher or other specialized courses so they will remain proficient and knowledgeable concerning unusual or new technical penetration techniques.

9. TSCM Equipment Development, Procurement, and Disposal. The hostile technical threat is assumed to be essentially the same for all DoD Components. Therefore, the best possible defense for all DoD Components shall be to work together and have commonality of TSCM equipment consistent with the latest technical developments of such equipment.

a. The TSCM program managers shall monitor closely the research, development, testing, evaluation, and procurement of TSCM equipment to ensure greatest integration, standardization, and compatibility.

b. The inter-Service transfer of excess TSCM equipment is encouraged. TSCM equipment declared obsolete and identified for disposal action shall be demilitarized if the equipment reveals or tends to reveal countermeasures capabilities or limitations.

10. Cross-Servicing of TSCM Support. Achieving commonality on the conduct of technical services, training, and equipment increases the potential for cross-servicing of TSCM services among the DoD Components. The TSCM program manager for each DoD Component shall facilitate DoD Component-level coordination in all TSCM matters on personnel, equipment, standards of performance, and cross-servicing. Cross-servicing agreements for TSCM support shall be developed by DoD Components in all areas where economically feasible. This service will be provided on a nonreimbursable basis.

F. RESPONSIBILITIES

1. The Deputy Under Secretary of Defense for Policy, under DoD Directive 5111.1 (reference (g)), shall provide DoD policy and oversee the TSCM survey program.

2. The Secretaries of the Military Departments and the Directors, National Security Agency/Chief, Central Security Service; Defense Intelligence Agency, and Washington Headquarters Services, or designees, shall:

- a. Establish a centrally managed TSCM survey program.
- b. Appoint a TSCM program manager who shall serve as their Component focal point for managing the TSCM survey program.

3. Heads of DoD Components, or designees, shall comply with the provisions of this Instruction and shall:

- a. Coordinate proposed TSCM equipment development and acquisition activities through the DUSD(P) and existing and appropriate subcommittees under the DCI Security Committee (SECOM).

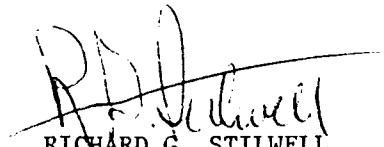
May 23, 84
5240.5

b. Coordinate with the DUSD(P) and the appropriate SECOM subcommittee requests by foreign agencies for the release of TSCM equipment and techniques and obtain their concurrence before taking any action on such requests.

c. Ensure that their TSCM personnel attend refresher or other specialized courses periodically (see paragraph E.8.b., above).

G. EFFECTIVE DATE AND IMPLEMENTATION

This Instruction is effective immediately. Forward two copies of implementing documents to the Deputy Under Secretary of Defense for Policy with 120 days.



RICHARD G. STILWELL
General, USA (Ret.)
Deputy Under Secretary of Defense
for Policy

Enclosures - 3

1. Qualifications for Entry into TSCM Support Field
2. DoD Classified Presentations at Congressional Activities
3. Information for Technical Security Survey Report

QUALIFICATION FOR ENTRY INTO TSCM FIELD

The minimum qualifications required for entry into the TSCM field are as follows:

1. Education. Completion of high school or equivalent and completion of a comprehensive course in electronics fundamentals.
2. Experience. The TSCM applicant must be certified by the DoD Component concerned and authorized as qualified to perform TSCM functions at the professional level.
3. Clearance. Each TSCM representative must undergo a thorough background investigation to qualify for all special clearances required to permit access to those areas requiring technical security services.
4. Grade. E-5 or higher, or an equivalent civilian position.
5. Physical. The TSCM representative shall be physically fit and meet the physical standards set forth by each DoD Component.

Accession For	
NTIS GRA&I	✓
DTIC TAB	
Unannounced	
Justification	
By <i>form 50</i>	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

DTIC QUALITY INSPECTED 8

May 23, 84
5240.2 (Encl 2)

DOD CLASSIFIED PRESENTATIONS AT CONGRESSIONAL
ACTIVITIES

1. The Department of the Army shall provide technical surveillance counter-measure (TSCM) support for DoD appearances before members of Congress and congressional staff when classified presentations are made. Requests for this support shall be made directly to the Department of the Army Intelligence and Security Command Legislative Support Office. Requests shall be made as far in advance as possible to allow effective scheduling of TSCM assets. The requests must be classified SECRET.
2. If a technical hazard or penetration is discovered, the TSCM special agent shall inform those concerned and recommend that the presentation be suspended until the hazard or penetration is identified and eliminated.

INFORMATION FOR TECHNICAL SECURITY SURVEY REPORT¹

Reports shall be prepared in enough copies to allow distribution to requestors, monitoring agencies, and the responsible DoD Component TSCM program manager. At a minimum, they shall contain the following information:

1. Unit identification and geographical location (also account number if National Communications Security Instruction survey).
2. Who requested the survey.
3. When was it accomplished.
4. Description of support provided. Describe briefly if a complete TSCM survey, monitor, or other TSCM activity was performed.
5. Findings. If security vulnerabilities or hazards are discovered, report them in detail.
6. Recommendations. For each vulnerability or hazard reported, how to eliminate or correct the deficiency. Written recommendations shall be evaluated carefully whether they will correct effectively the noted deficiency and the cost of implementation.
7. Name or names of the local person or persons briefed on the results of the TSCM activity.

¹This information shall be classified under subsection E.7., basic Directive.